ADVISORY NUMBER:
SA2016-021

DATE(S) ISSUED:
01/29/2016

SUBJECT:
A Vulnerability in GNU C Library Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in the GNU C Library (glibc) which could
allow for arbitrary code execution. This library is required in all modern
distributions of Linux as it defines the system calls and other basic facilities
used in the Linux kernel. Successful exploitation of this vulnerability could
result in an attacker gaining the same privileges as the exploited
application. Depending on the privileges associated with the application, an
attacker could then install programs; view, change, or delete data; or create
new accounts with full user rights. Failed exploit attempts could lead to a
denial of service condition for the affected application.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the
wild. However, a proof of concept exploit has been publically released.

SYSTEMS AFFECTED:
GNU glibc prior to version 2.23, found in (but not limited to) the following systems:

- Caldera OpenLinux Server

- Caldera OpenLinux Workstation

- Connectiva Linux

- Debian Linux

- EnGarde Secure Linux Secure Linux

- Gentoo Linux

- HP Secure OS software for Linux

- Mandriva apcupsd

- Mandriva Corporate Server

- Mandriva Linux Mandrake

- Mandriva Single Network Firewall

- Openwall

- Redhat Enterprise Linux AS

- Redhat Enterprise Linux AS

- Redhat Enterprise Linux ES

- Redhat Enterprise Linux ES

- Redhat Enterprise Linux WS

- Redhat Enterprise Linux WS

- Redhat Fedora Core2

- Redhat Linux

- Redhat Linux Advanced Work Station

- Slackware Linux

- Sun Linux

- SuSE Linux

- SuSE Linux Database Server

- SuSE Linux Enterprise Server for S/390

- SuSE Linux Firewall on CD

- SuSE SuSE eMail Server III

- SuSE SUSE Linux Enterprise Server

- Trustix Secure Linux

- Trustix Secure Linux

- Ubuntu Ubuntu Linux

- WireX Immunix OS

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

A stack-based buffer overflow vulnerability has been discovered in GNU libc that could allow remote code execution on the affected device. Specifically, this vulnerability affects the 'catopen()' function in libc where it fails to properly bound-check user-supplied data. This vulnerability can be exploited when the system processes maliciously crafted data. (CVE-2015-8779)

An attacker can exploit this vulnerability to execute arbitrary code in the context of the affected application. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the exploited application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts could lead to a denial of service condition for the affected application.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by the affected *nix distribution to the vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Sourceware:
https://sourceware.org/bugzilla/show_bug.cgi?id=17905

Redhat:
https://bugzilla.redhat.com/show_bug.cgi?id=1300312

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8779